BELKIN | OmniView®

Belkin OmniView® Secure KVM Switch User Manual F1DN102U F1DN104U F1DN108U Common Criteria supplement

This section supplements the Belkin Quick Installation Guide in accordance with ADO_IGS.1 Common Criteria Assurance Measure requirements.

This User Guidance and Common Criteria EAL 4 validation apply to the TOE Common Criteria Evaluated version of OmniView™ Secure KVM Models listed below:

F1DN102U Version v.321211

F1DN104U Version v.321211

F1DN108U Version v.321211

Before you begin: The Users of the Belkin OmniView™ Secure KVM must review all associated documentation and guidance, prior to proceeding with installation and use of the KVM switch.

1.1 Receipt and preparation of TOE and Environment prior to installation

Receipt

- Assure that tamper seals are intact on the KVM switch.

Environment preparation

- The Belkin OmniView KVM secure must be located in a physically secure location providing physical protection and limited (authorized user) access controls.

1.2 Verification of Common Criteria components

The following are authorized devices for the Common Criteria Evaluated configuration. Assure that installation processes resulting in the following hardware/firmware configuration:

TOE	Belkin Secure KVM Switch 2 Port PN # F1DN102U v.321211 (or) Belkin Secure KVM Switch 4 Port PN # F1DN104U v.321211 (or) Belkin Secure KVM Switch 8 Port PN # F1DN108U v.321211 (and) Firmware Version 3.16
Environment	USB Mouse (Peripheral Group Member)
Environment	USB Keyboard (Peripheral Group Member)
Environment	Monitor – VGA connector (Peripheral Group Member)
Environment	Host Computers Qty 2, 4 or 8 based on KVM used (IT Environment Computer resources)

1.3 Usage Assumptions

The Common Criteria Evaluated Configuration requires the following assumptions in usage of the OmniView Secure KVM device. These assumptions should be assured either through facility or procedural provisions.

- An AUTHORIZED USER possesses the necessary privileges to access the information transferred by the TOE.
- USERS are AUTHORIZED USERS.
- The TOE meets the appropriate national requirements (in the country where used) for conducted/radiated electromagnetic emissions. [In the United States, Part 15 of the FCC Rules for Class B digital devices.]
- Only the selected COMPUTER'S video channel will be visible on the shared MONITOR.
- The TOE is installed and managed in accordance with the manufacturer's directions.
- The AUTHORIZED USER is non-hostile and follows all usage guidance.
- The TOE is physically secure.
- Vulnerabilities associated with attached DEVICES (SHARED PERIPHERALS or SWITCHED COMPUTERS), or their CONNECTION to the TOE, are a concern of the application scenario and not of the TOE.

2. Common Criteria Administrative Guidance - OmniView® Secure KVM Switch User Manual F1DN102U F1DN104U F1DN108U

The follow section lists the supplemental information relating to a Common Criteria deployment for the OmniView® Secure KVM Switch User Manual in accordance with AGD_USR.1 & AGD_ADM.1 Common Criteria Assurance Measure requirements.

Usage Assumptions

Note that the usage assumptions listed in Section 1.3 must be maintained to assure all TOE security objectives are maintained during usage.

Applicability of OmniView® Secure KVM Switch User Manual to Common Criteria

The OmniView Secure KVM Switch User Manual applies in its entirety to the Common Criteria Evaluated Configuration.